恶意代码分析

2020年8月23日 15:19

1. 蠕虫
    a. 和病毒
        i. 本质上是相关的，开始蔓延时都是自我复制
        ii. 蠕虫特征是通过网络传输，而病毒不一定要通过网络传播
        iii. 病毒特征是感染主文件，而蠕虫不一定要宿主文件
        iv. 蠕虫无须人为干预传播，通常利用目标机上的漏洞能自动化地占据，而大多数病毒需要用户运行程序或打开文档以调用恶意代码
2. 木马
    a. 和后门
        i. 仅提供远程访问的程序只是后门
        ii. 被伪装成良性程序时是木马
        iii. 木马常伪装后门，使木马控制着能登录被感染计算机
        iv. 木马也可以用于发起DOS
        v. 木马还可能隐藏恶意进程的痕迹、收集信息